Список литературы

1. Технология изготовления печатных плат : [учеб. пособие] / Л.А. Брусницына, Е.И. Степановских ; [науч. ред. В.Ф. Марков] ; М-во образования и науки Рос. Федерации, Урал. федер. ун-т. — Екатеринбург : Изд-во Урал. ун-та, 2015. — 200 с.

2. Встраивание пассивных и активных компонентов в печатные платы – альтернатива печатному монтажу. Научный журнал «Новые Технологии», №6 январь 2011 – 92 с.

3. Васильев А.Н., Овчинников В.А., Лебедев В.В. Проектирование печатных плат: Учебное пособие. 1-е изд. Тверь: ТГТУ, 2005. 116 с.

А.А. Бондюгин, А.А. Боярская, С.А. Шарапов
Уральский федеральный университет имени первого Президента России Б. Н. Ельцина
Екатеринбург, Россия

Исследование средств тестирование систем на устойчивость к (D) DoS-атакам

В статье рассмотрены основные инструменты для проведения тестирования информационных сервисов на устойчивость к (D)DoS-атакам. Проведено исследование наиболее эффективных и универсальных средств.

(D) DoS-testing

A Denial-of-Service (DoS) attack is an attack in which one or more machines target a victim and attempt to prevent the victim from doing useful work. The victim can be a network server, client or router, a network link or an entire network, an individual Internet user or a company doing business using the Internet, an Internet Service Provider, country, or any combination of or variant on these.

Almost all Internet services are vulnerable to denial-of-service attacks of sufficient scale. In most cases, sufficient scale can be achieved by compromising enough end-hosts (typically using a virus or worm) or routers, and using those compromised hosts to perpetrate the attack. Such an attack is known as a Distributed Denial-of-Service (DDoS) attack. However, there are also many cases where a single well-connected end-system can perpetrate a successful DoS attack [2].

DoS and DDoS pose a significant risk to critical infrastructure and business entities. (D)DoS Testing will show whether your system is well protected, and how you can protect it.

(D) DoS attacks can be divided into the following categories:

- attacks operating at the application layer, using features of a specific application;
- attacks that use host layers protocols of the network model;
- attacks operating at the media layers of the network model, aimed at reducing the channel capacity.

Testing Tools can be classified as follows:

- Hardware and software systems, such as IXIA, Spirent, and so on. This solution is effectively and provides detailed reports and statistics at the output, but it is very expensive and it has poor scalability. It can be used in large companies.
- Tools, what we can find in special Linux distributions (especially - Kali Linux). It is free and universal solution. It is described in table 1.
- Software solutions, for example, WAF Testing Framework by Imperva and Akamai. It is also quite expensive.
- Vulnerability scanners, which allow to simulate the attacks. This solution has limited functionality.
- Amateur tools. Such tools are easy to use. It is possible to overwatch the reaction of the test object, but it is impossible to have output statistics.

Table 1 – Kali Linux tools

Title	Description
SlowHTTPTest	• SlowHTTPTest is a highly configurable tool that simulates some Application Layer Denial of Service attacks; • It works on majority of Linux platforms, OSX and Cygwin – a Unix-like environment and command-line interface for Microsoft Windows;

	• Depending on the level of detail, the output can be simple, as generated messages every 5 seconds, and full, as traffic dump.
GoldenEye	• Implements HTTP-flood (GET and POST); • Each GET request contains different line, different user agents and different referee, including Bing, Baidu, Yandex and other search engines, so the server transmits traffic with code 200 (OK).
Hping3	• It works well if there are other running DoS tools such as GoldenEye on your computer; • It is a free packet generator and analyzer for the TCP / IP protocol (it implements SYN-flooding attacks, TCP connects) [1].

The simulation DDoS tools of KaliLinux 2.0 were tested experimentally. The scheme of test stand is shown in figure 1.

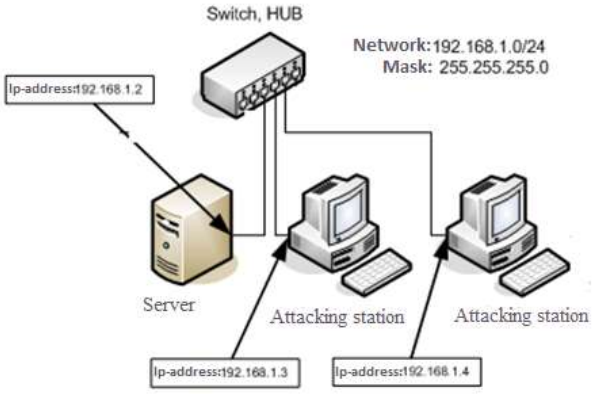

Figure 1 - The scheme of test stand

The PC was as a server (the object of attack), with the operating system UbuntuServer 12.0, Apache Web Server was installed on it. The two PC were as attacking stations with operating systems KaliLinux 2.0 and Windows 8.

First of all, Hping3 utility has been tested. For example, we have used the following situation. The following command starts hping3:

- *root@WebWare-Kali:~# hping3 -c 10000 -d 120 -S -w 64 -p 21 --flood --rand-source 192.168.1.2.*

Let's look at the situation from the server. The state of the server after the start attack is shown in figure 2. We can see that the processor is loaded with 95 percent.

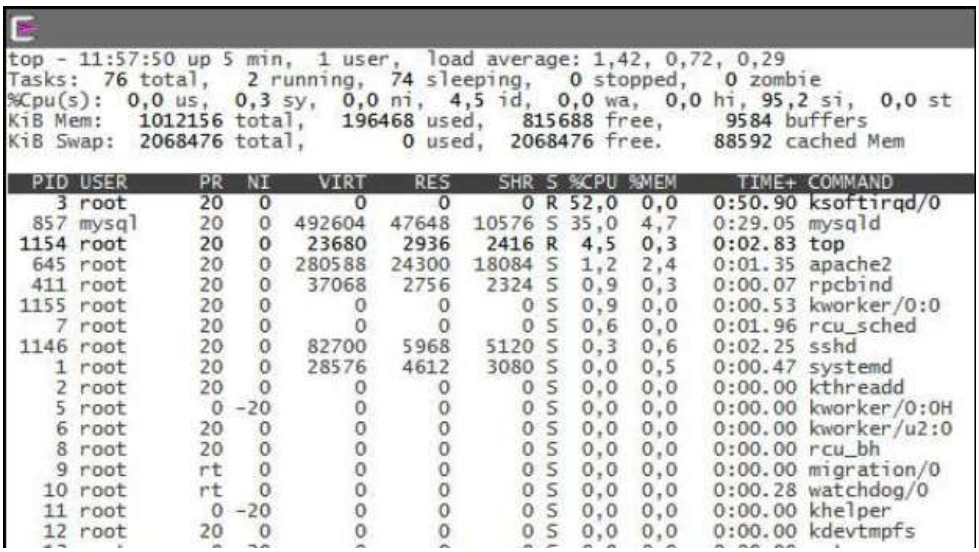

Figure 2 - The state of the server Hping3

Then, GoldenEye has been tested. The program starts with the following command:

- *./goldeneye.py http://192.168.1.2/info.php*

Let's look at the state of the server (figure 3). In this case, the processor is still practically inactive, but the amount of free memory reduced, in addition, the number of sleeping processes increased.

As a result of logs analysis we can see different strings, different user agents and a variety referee in GET request. When the Web server meets this attack, it analyzes the entering traffic, checks the requested URL, the source address and «Referrer» field. Then, it skips them with code 200 OK.

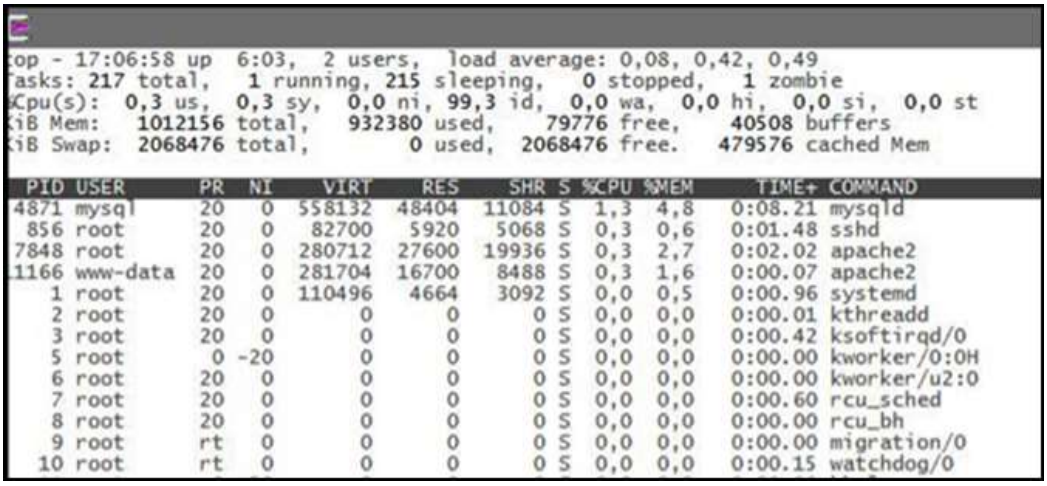

Figure 3 - The state of the server GoldenEye

Thirdly, SlowHTTPTest has been tested. It takes all available connection pool. Attacks Slowloris and Slow HTTP POST occupy server resources and cause a denial of service by slow retrieving or sending the request.

For example:

- *slowhttptest -c 1000 -H -i 10 -r 200 -t GET -u http://192.168.1.37/info.php -x 24 -p 3:.*

Let's look at the state of the server, in fact, at the state of RAM (figure 4). We can see that the amount of memory was reduced very quickly. The server went down and levelled off (figure 5).

```
root@WebWare-Debian:~# free
             total       used       free     shared    buffers     cached
Mem:       1012156     651984     360172       9912      37960     476428
-/+ buffers/cache:     137596     874560
Swap:      2068476          0    2068476
root@WebWare-Debian:~# free
             total       used       free     shared    buffers     cached
Mem:       1012156     828352     183804       9912      37968     476428
-/+ buffers/cache:     313956     698200
Swap:      2068476          0    2068476
root@WebWare-Debian:~# free
             total       used       free     shared    buffers     cached
Mem:       1012156     845908     166248       9912      37968     476428
-/+ buffers/cache:     331512     680644
Swap:      2068476          0    2068476
root@WebWare-Debian:~# free
             total       used       free     shared    buffers     cached
Mem:       1012156     845988     166168       9912      37968     476428
-/+ buffers/cache:     331592     680564
Swap:      2068476          0    2068476
root@WebWare-Debian:~# free
             total       used       free     shared    buffers     cached
Mem:       1012156     846084     166072       9912      37968     476428
-/+ buffers/cache:     331688     680468
Swap:      2068476          0    2068476
root@WebWare-Debian:~#
```

Figure 4 - The state of the server's RAM

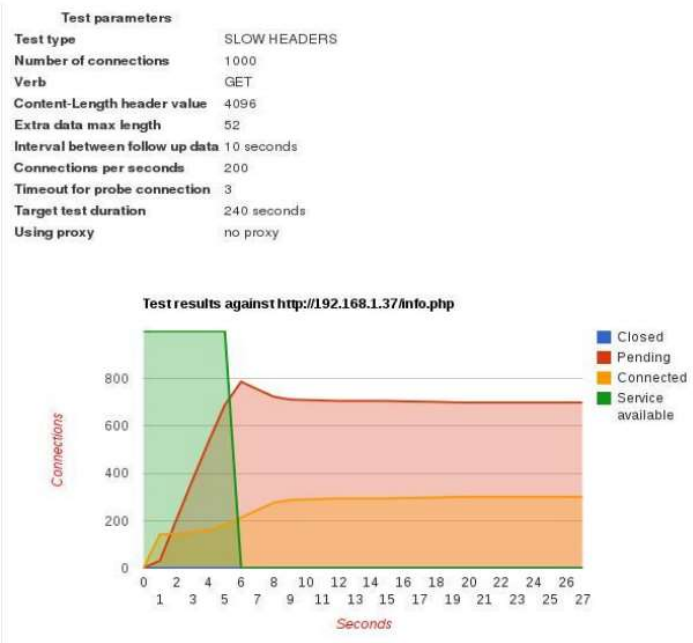

Figure 5 - Report about the work of program

So, the existing (D)DoS-testing tools have been reviewed and conducted. It has been found that these tools can be used to create scalable

network services. For example, it is possible to use cloud computing power to create such services.

Список литературы:

1. Милосердов А.В. Тестирование на проникновение с помощью Kali Linux/M.: Webware.biz, 2015.
2. Handley M., Rescorla E., Internet Denial-of-Service Considerations (RFC 4732)/ The IETF Trust, 2006.

Е.Ф. Запольских, Е.В. Прокопенко
Уральский федеральный университет имени первого Президента России Б.Н. Ельцина
Екатеринбург, Россия

Пространственно-временная модель сигнала радиовысотомера с ЛЧМ при отражении от морской поверхности

В статье рассматриваются особенности моделирования отражённого сигнала радиовысотомера над морской поверхностью при различной высоте волн, введении углов эволюции и скорости летательного аппарата, а также изменении ширины диаграммы направленности антенны. Произведено краткое описание влияющих факторов, которые были учтены при моделировании работы радиовысотомера. Дан анализ результатов моделирования.

Space-time model of radio altimeter LFM signal reflected from the sea surface

Currently, modern computational power allows implementing quite plausible ways to simulate signals reflected from different objects. Besides